

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X

ELEKTRA ENTERTAINMENT GROUP INC., a Delaware :
corporation; UMG RECORDINGS, INC., a Delaware
corporation; and VIRGIN RECORDS AMERICA, INC., a :
California corporation,

Plaintiffs,

-against-

DENISE BARKER,

Defendant.

Case No. 05CV7340(KMK)(THK)

:

:

:

:

-----X

**PLAINTIFFS' BRIEF IN RESPONSE TO THE
AMICUS CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION**

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
INTRODUCTION	1
ARGUMENT	2
I. BECAUSE THE ISSUES RAISED BY THE EFF WERE NOT RAISED BY ANY OF THE PARTIES IN THIS CASE, THIS COURT SHOULD NOT CONSIDER THOSE ISSUES.	2
II. SHOULD THE COURT CONSIDER THE ISSUE RAISED BY THE EFF, THE COURT SHOULD FOLLOW THE VAST MAJORITY OF COURTS AND COMMENTATORS AND FIND THAT THE UNAUTHORIZED DISTRIBUTION OF COPYRIGHTED SOUND RECORDINGS OVER P2P NETWORKS VIOLATES THE EXCLUSIVE RIGHT OF DISTRIBUTION	3
A. The Language of the Copyright Act Subsumes the Unauthorized Distribution of Electronic Files Over P2P Networks.....	3
B. Adopting the EFF’s Position Would Improperly Render Various Provisions of the Copyright Act Meaningless	4
C. Every Court That Has Addressed the Issue, Including the United States Supreme Court and This Court, As Well As Most Commentators, Has Found That the Unauthorized Transmission of Electronic Files Containing Copyrighted Works Violates the Exclusive Right of Distribution	5
D. The Legislative History on Which the EFF Relies Does Not Support the EFF’s Position.....	8
1. The Legislative History Underlying the Copyright Act of 1976 Does Not Address The Issue Before This Court.....	9
2. The NII White Paper And The Legislative History Of The 1995 Act Support Plaintiffs’ Position Here	9
CONCLUSION.....	10

TABLE OF AUTHORITIES

CASES

<u>A&M Records, Inc. v. Napster, Inc.</u> , 239 F.3d 1004 (9 th Cir. 2001)	6
<u>A.D. Bedell Wholesale Co. v. Philip Morris Inc.</u> , 263 F.3d 239 (3d Cir. 2001), <u>cert. denied</u> , 534 U.S. 1081 (2002).....	2
<u>Agee v. Paramount Comms., Inc.</u> , 59 F.3d 317 (2 nd Cir. 1995).....	7, 8
<u>Bano v. Union Carbide Corp.</u> , 273 F.3d 120 (2d Cir. 2001)	2
<u>Eldred v. Ashcroft</u> , 255 F.3d 849 (D.C. Cir. 2001)	2
<u>General Eng'g Corp. v. Virgin Islands Water & Power Auth.</u> , 805 F.2d 88 (3d Cir. 1986)	2
<u>Getaped.com, Inc. v. Cangemi</u> , 188 F. Supp. 2d 398 (S.D.N.Y. 2002).....	7
<u>In re Aimster Copyright Litigation</u> , 334 F.3d 643 (7 th Cir. 2003), <u>cert. denied</u> , 540 U.S. 1107 (2004).....	6
<u>In re Verizon Internet Services, Inc.</u> , 240 F. Supp. 2d 24 (D.D.C.), <u>rev'd on other grounds</u> , 351 F.3d 1229 (D.C.C. 2003), <u>cert. denied</u> , 543 U.S. 924 (2004).....	2
<u>MAI Systems Corp. v. Peak Computer, Inc.</u> , 991 F.2d 511 (9 th Cir. 1993), <u>cert. dismissed</u> , 510 U.S. 1033 (1994).....	4
<u>Marobie-FL, Inc. v. Nat'l Ass'n of Fire & Equip. Distribs. & Northwest Nexus, Inc.</u> , 983 F. Supp. 1167 (N.D. Ill. 1997).....	7
<u>Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.</u> , 125 S. Ct. 2764 (2005)	6
<u>Michaels v. Internet Entm't Group, Inc.</u> , 5 F. Supp. 2d 823 (C.D. Cal. 1998).....	7
<u>New York Times Co. v. Tasini</u> , 533 U.S. 483 (2001)	6
<u>Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.</u> , 939 F. Supp. 1032 (S.D.N.Y. 1996)	7
<u>Playboy Enterprises, Inc. v. Frena</u> , 839 F. Supp. 1552 (M.D. Fla. 1993).....	6, 7
<u>Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.</u> , 982 F. Supp. 503 (N.D. Ohio 1997)	7
<u>Playboy Enterprises, Inc. v. Webbworld, Inc.</u> , 991 F. Supp. 543 (N.D. Tex. 1997), <u>aff'd</u> , 168 F.3d 486 (5 th Cir. 1999)	7
<u>Reiter v. Sonotone Corp.</u> , 442 U.S. 330 (1979).....	4
<u>Religious Tech. Ctr., Inc. v. Netcom On-Line Comm. Servs., Inc.</u> , 907 F. Supp. 1361 (N.D. Cal. 1995).....	7
<u>Stenograph L.L.C. v. Bossard Assocs., Inc.</u> , 144 F.3d 96 (D.C. Cir. 1998).....	4

STATUTES

17 U.S.C. § 106(1)	4
17 U.S.C. § 106(3)	3, 6, 8, 9
17 U.S.C. § 114(b)	5
17 U.S.C. § 512(a)	5

OTHER AUTHORITIES

4 AM. JUR. 2d <u>Amicus Curiae</u> §§ 6, 7 (2004)	2
DMCA Section 104 Report, available at < http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf	7
<u>Final Report of the National Commission on New Technological Uses of Copyrighted Works</u> , H.R. Rep. No. 1307, 96 th Cong., 1 st Sess., at 22, <u>reprinted</u> in 1980 U.S.C.C.A.N. 6460 (1980).....	4
Fred von Lohmann, <u>Peer-to-Peer File Sharing and Copyright Law after Napster</u> , < http://www.mp3offshore.comcopyrightlaw.html > (Jan. 2003)	1, 2, 4, 7
H.R. Rep. No. 1476, 94 th Cong., 2d Sess. 138, <u>reprinted</u> in 1976 U.S.C.C.A.N. 5659, 5754	9
Keith Kupferschmid, <u>Lost in Space: The Digital Demise of the First-Sale Doctrine</u> , in 16 J. MARSHALL J. COMPUTER & INFO. L. 825 (Summer 1998)	3, 4
Niels Schaumann, <u>Copyright Infringement and Peer-to-Peer Technology</u> , in 28 WM. MITCHELL L. REV. 1001, 1037 (2002)	3, 4
NII White Paper	8, 9
S. 128, 104 th Cong., 1 st Sess. 27 (1995), <u>reprinted in</u> 1995 U.S.C.C.A.N. 356, 374	10

Plaintiffs Elektra Entertainment Group Inc., UMG Recordings, Inc., and Virgin Records America, Inc. (“plaintiffs”) respectfully submit this response to the amicus curiae brief of the Electronic Frontier Foundation (“EFF”).¹

INTRODUCTION

The EFF’s amicus brief seeks to have this court rule that one of the fundamental rights of a copyright owner, the exclusive right of distribution, does not apply on the Internet. Needless to say, the consequences of such a decision would be dramatic. It would literally unwind the basic structure of copyright laws as applied to a medium that has become fundamental in this nation’s economy.

The EFF’s argument is that the language of the Copyright Act covers distribution of copyrighted works only if tangible materials are transferred. The EFF has misinterpreted the statute and the legislative history. Indeed, its argument fails to acknowledge that the vast majority of courts, if not every court, that has addressed this issue has rejected it and found, either directly or implicitly, that the transmission of electronic files from one person to another does implicate the exclusive right of distribution set forth in the Copyright Act. Moreover, the EFF has failed to explain how the remainder of the copyright statute can be interpreted to make sense if it is correct about the limitations of the right of distribution. Finally, the EFF has overlooked its own 2003 analysis of the issue, in which it concluded that “the transmission of a file from one person to another results in a reproduction, a distribution, and possibly a public performance” under the Copyright law. See Fred von Lohmann, Peer-to-Peer File Sharing

¹ Plaintiffs note that, this morning, defendant filed a pleading commenting on the EFF’s amicus brief. This pleading was filed without authorization and should be stricken. In any event, defendant’s statement that plaintiffs failed to allege improper reproduction or distribution is false. See, e.g., Compl. ¶ 12.

and Copyright Law after Napster, <<http://www.mp3offshore.com/copyrightlaw.html>> (Jan. 2003) (hereafter “von Lohmann”) (a copy of this article is attached as Appendix A).

ARGUMENT

I. BECAUSE THE ISSUES RAISED BY THE EFF WERE NOT RAISED BY ANY OF THE PARTIES IN THIS CASE, THIS COURT SHOULD NOT CONSIDER THOSE ISSUES.

It is well-settled that new issues raised by an amicus and that were not raised by any of the parties generally are not properly before the court. See Bano v. Union Carbide Corp., 273 F.3d 120, 127 n. 5 (2d Cir. 2001) (refusing to consider issues raised only by amici but not by the parties themselves); A.D. Bedell Wholesale Co. v. Philip Morris Inc., 263 F.3d 239, 266 (3d Cir. 2001), cert. denied, 534 U.S. 1081 (2002); Eldred v. Ashcroft, 255 F.3d 849, 851 (D.C. Cir. 2001); General Engineering Corp. v. Virgin Islands Water & Power Authority, 805 F.2d 88, 92 n. 5 (3d Cir. 1986) (collecting cases); In re Verizon Internet Services, Inc., 240 F. Supp. 2d 24, 42 (D.D.C.), rev'd on other grounds, 351 F.3d 1229 (D.C.C. 2003), cert. denied, 543 U.S. 924 (2004); 4 Am. Jur. 2d Amicus Curiae §§ 6 (“An amicus curiae is not a party and generally cannot assume the functions of a party, or an attorney for a party.”), 7 (“In general, an amicus curiae must accept the case before the court with the issues made by the parties. Accordingly, an amicus curiae ordinarily cannot inject new issues into a case which have not been presented by the parties.”) (2004) (footnotes omitted).

Here, the EFF seeks to have the Court rule that the exclusive right of distribution does not cover digital transmissions. This argument cannot be found in any form or function in the defendant’s motion to dismiss. It was not raised by any party in this case and is only now before the Court by virtue of the EFF’s amicus brief. Because it is improper for an amicus to introduce

new issues that have not been raised by any party, this Court should not consider the issues raised in the EFF's brief.

II. SHOULD THE COURT CONSIDER THE ISSUE RAISED BY THE EFF, THE COURT SHOULD FOLLOW THE VAST MAJORITY OF COURTS AND COMMENTATORS AND FIND THAT THE UNAUTHORIZED DISTRIBUTION OF COPYRIGHTED SOUND RECORDINGS OVER P2P NETWORKS VIOLATES THE EXCLUSIVE RIGHT OF DISTRIBUTION

A. The Language of the Copyright Act Subsumes the Unauthorized Distribution of Electronic Files Over P2P Networks

17 U.S.C. § 106(3) grants to a copyright owner the exclusive right to distribute copies or phonorecords of a copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending. As such, the Copyright Act grants a copyright holder, among other rights, the exclusive right to transfer, but it does not require that such transfer involve the movement of any particular material object from one computer to another. Rather, the Act requires only that a material object embodying a copyright owner's work be delivered into someone else's hands or computer hard drive, as the case may be. In other words, the statute requires only that, at the end of the transaction, a work is transferred from one location to another, not whether a material object has been transferred. This distinguishes the distribution right from the public display and performance rights set forth elsewhere in § 106. Simply stated, as long as the recipient of the work being transmitted has a material object embedded with the work after a transfer has taken place, a distribution has occurred. See Keith Kupferschmid, Lost in Space: The Digital Demise of the First-Sale Doctrine, 16 J. Marshall J. Computer & Info. L. 825, 849-50 (Summer 1998) (hereafter "Kupferschmid"); accord Niels Schaumann, Copyright Infringement and Peer-to-Peer Technology, 28 Wm. Mitchell L. Rev. 1001, 1037 (2002) (hereafter "Schaumann").

To argue that a distribution must involve the transfer of tangible objects simply ignores the reality of electronic transmissions, which, when they result in identifiable fixations on a recipient's computer, are the functional equivalent of receiving a tangible copy. Arguing that such a transmission does not amount to a distribution needlessly, and inconsistent with the Copyright Act, anchors the concept to distribution to the long past, when the only way copies could be distributed was through the dissemination of tangible objects. See Schaumann, at 1037.

This analysis is fully consistent with the well-established view that the unlawful downloading of a copyrighted work to one's computer violates the exclusive right of reproduction set forth in 17 U.S.C. § 106(1). The EFF apparently concedes, as it must, that an MP3 file residing on a downloader's computer constitutes a copy or phonorecord and, thus, by definition, is a "material object" under § 101 of the Copyright Act. See von Lohmann, at 3 (App. A); see also Stenograph L.L.C. v. Bossard Associates, Inc., 144 F.3d 96, 101-02 (D.C. Cir. 1998) (reproduction of program in random access memory creates a "copy"); MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994) (same); Final Report of the National Commission on New Technological Uses of Copyrighted Works, H.R. Rep. No. 1307, 96th Cong., 1st Sess., at 22, reprinted in 1980 U.S.C.C.A.N. 6460 (1980) ("Because works in computer storage may be repeatedly reproduced, they are fixed and, therefore, are copies."); Kupferschmid, at 842-43. For the same reasons that an MP3 file residing on a downloader's computer is a copy of a phonorecord for purposes of the Act, the unauthorized transmittal of such a file over P2P networks satisfies the requirements of distribution under the Act.

B. Adopting the EFF's Position Would Improperly Render Various Provisions of the Copyright Act Meaningless

It is a settled principle of statutory construction that courts must construe statutory schemes so as to give effect to all provisions of a statute. See, e.g., Reiter v. Sonotone Corp., 442 U.S. 330, 339 (1979). Here, adopting the position that the EFF espouses would improperly render several clauses of the Copyright Act meaningless.

For example, section 512 of the Digital Millennium Copyright Act limits the liability of, among others, Internet service providers for copyright infringement resulting from the use of their networks to infringe copyrights by transmitting copyrighted works without authorization. See 17 U.S.C. § 512(a). This provision necessarily assumes that distribution of electronic files over a network implicates the exclusive right of distribution. If the distribution of electronic files over a network could not violate the exclusive right of distribution, as the EFF claims, then there would be no reason for § 512(a).

Similarly, 17 U.S.C. § 114(b) provides, in relevant part, “The exclusive rights of the owner of copyright in a sound recording under clauses (1), (2), and (3) of section 106 [including the distribution right] do not apply to sound recordings included in educational television and radio programs . . . distributed or transmitted by or through public broadcasting entities” Again, if, as the EFF contends, the right of distribution does not protect electronic transmissions, then there would be no need for this sentence, because the distribution right could never apply to transmissions by or through public broadcasting entities.

For all of the foregoing reasons, the EFF’s interpretation of the distribution right would render meaningless several provisions of the Copyright Act. Because a court must always construe a statutory scheme to give meaning to all of its provisions, the EFF’s interpretation should be rejected.

C. Every Court That Has Addressed the Issue, Including the United States Supreme Court and This Court, As Well As Most Commentators, Has

Found That the Unauthorized Transmission of Electronic Files Containing Copyrighted Works Violates the Exclusive Right of Distribution

Consistent with the interpretation of the Copyright Act set forth above, every court of which plaintiffs are aware, including the Supreme Court and this Court, have concluded that the unauthorized transmission of electronic files over the Internet and over P2P networks implicates the exclusive right of distribution. In New York Times Co. v. Tasini, 533 U.S. 483, 498 (2001), the United States Supreme Court found a violation of the exclusive right of distribution where copyrighted news articles were uploaded to electronic and CD-ROM databases and publicly distributed through the NEXIS database. A fundamental presumption in the Supreme Court's analysis is that the § 106(3) right encompasses digital transmissions.

Similarly, last year, in Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005), the Supreme Court considered the issue of whether propagators of P2P file-sharing software could be secondarily liable for the direct infringements of their users. The Court found that they could. See id. at 2782. Fundamental to the Court's conclusion was that the underlying electronic transmissions violated the distribution right. See id. ("MGM's evidence in this case most obviously addresses a different basis of liability for distributing a product open to alternative uses. Here, evidence of the distributors' words and deeds going beyond distribution as such shows a purpose to cause and profit from third-party acts of copyright infringement. If liability for inducing infringement is ultimately found, it will not be on the basis of presuming or imputing fault, but from inferring a patently illegal objective from statements and actions showing what that objective was."); accord In re Aimster Copyright Litigation, 334 F.3d 643, 645 (7th Cir. 2003), cert. denied, 540 U.S. 1107 (2004) (holding that file-swapping, which involves the making and transmitting of a digital copy of music, infringes copyrights); A&M

Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001) (“Napster users who upload file names to the search index for others to copy violate plaintiffs’ distribution rights.”).

Every other court of which plaintiffs are aware is in accord. For example, in Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993), the court found that the operator of a subscription computer billboard whose service was used by subscribers to transmit unauthorized copies of the plaintiff’s copyrighted work violated the exclusive right of distribution. Although the EFF seeks to ignore this decision because it lacks detailed analysis, the fact is that numerous courts, including this Court and the U.S. Copyright Office, have reached the same conclusion. See, e.g., Getaped.com, Inc. v. Cangemi, 188 F. Supp. 2d 398, 402 (S.D.N.Y. 2002); Michaels v. Internet Entertainment Group, Inc., 5 F. Supp. 2d 823, 830-31 (C.D. Cal. 1998); Marobie-FL, Inc. v. National Association of Fire & Equipment Distributors & Northwest Nexus, Inc., 983 F. Supp. 1167, 1180 (N.D. Ill. 1997); Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 513 (N.D. Ohio 1997); Playboy Enterprises, Inc. v. Webbworld, Inc., 991 F. Supp. 543, 554 (N.D. Tex. 1997), aff’d, 168 F.3d 486 (5th Cir. 1999); Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc., 939 F. Supp. 1032, 1039 (S.D.N.Y. 1996); Religious Technology Center, Inc. v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995); DMCA Section 104 Report, at 79, available at <<http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf> (setting forth position of Copyright Office) (a copy of the relevant pages is attached as Appendix B). Indeed, as noted above, until now, the EFF itself had subscribed to this view. See von Lohmann, at 3 (App. A). The EFF should not now be heard to argue otherwise.

The Second Circuit’s decision in Agee v. Paramount Communications, Inc., 59 F.3d 317 (2nd Cir. 1995), on which the EFF relies, is inapposite. Agee involved a television station’s

transmission of a program for broadcast. On the facts before it, the court found that this transmission implicated the exclusive right of performance, as opposed to the exclusive right of distribution. See id. at 326. The Agee court expressly distinguished its facts from those at issue in Frena, and, as the EFF concedes, the Agee court did not even address the question of whether disseminations must always be in a physical form to constitute distribution under the Copyright Act. See Agee, 59 F.3d, at 325-26. In short, Agee did not address the issue that the EFF wishes to place before this Court and is irrelevant here.

Nor does the article by Professor Reese, on which the EFF's brief appears to be exclusively based, compel a different result. The fact is that, to plaintiff's knowledge, no court has ever adopted Professor Reese's analysis. To the contrary, as more fully set forth above, all courts that have addressed this issue have reached a contrary result.

For all of the foregoing reasons, because the vast majority of courts (if not all courts) that have addressed the issue before this Court have held that the unauthorized transmission of electronic files containing copyrighted works do, indeed, implicate the exclusive right of distribution, the EFF's contention that this Court should adopt a contrary position should be rejected.²

D. The Legislative History on Which the EFF Relies Does Not Support the EFF's Position

The EFF makes much of the legislative history underlying the 1976 Copyright Act, and the Digital Performance Right in Sound Recordings Act of 1995 (the "1995 Act"). The EFF also focuses on the so-called NII White Paper, in which the Clinton administration suggested that

² Plaintiffs note that the Department of Justice's well-publicized enforcement efforts against software piracy, which efforts have relied heavily on the distribution right, further support plaintiffs' position here.

17 U.S.C. § 106(3) should be amended to clarify that a transmission can constitute a distribution of copies or phonorecords of a work, which amendment was never adopted. The EFF's assertions are misplaced.

1. The Legislative History Underlying the Copyright Act of 1976 Does Not Address The Issue Before This Court

First, notwithstanding the EFF's assertions to the contrary, the legislative history underlying the Copyright Act of 1976 did not address the present issue, which involves a technology that did not then exist. The legislature did, however, attempt to distinguish the distribution right from the performance right, noting that, when a work is distributed, something must change hands. This is in contrast to transmissions of performances or displays (e.g., on television), in which nothing changes hands. See H.R. Rep. No. 1476, 94th Cong., 2d Sess. 138, reprinted in 1976 U.S.C.C.A.N. 5659, 5754. This view is entirely consistent with plaintiffs' position in this case. As noted above, transmissions of MP3 files over P2P networks result in the recipient's having a complete embodiment of the copyrighted sound recordings at issue. As such, something has changed hands, and pursuant to the 94th Congress's understanding of a distribution, the type of electronic transfer at issue here clearly satisfies that definition.

2. The NII White Paper And The Legislative History Of The 1995 Act Support Plaintiffs' Position Here

The EFF's effort to rely on the NII White Paper and the legislative history underlying the 1995 Act is equally unavailing. Indeed, both fully support plaintiffs' position here.

Although the EFF makes much of the fact that, in the NII White Paper, the Clinton administration encouraged Congress to amend 17 U.S.C. § 106(3) to clarify that electronic transmissions could implicate the distribution right, which Congress then failed to do, the EFF ignores the fact that the NII White Paper also stated that the proposed amendment was not

necessary, because the “existing right of distribution encompasses transmissions of copies.” NII White Paper, at 214.

Likewise, although the EFF notes that § 106(3) was not amended in connection with the 1995 Act, this fact is meaningless. The 1995 Act focused on performance rights, only. It did not address the distribution right. Notwithstanding that, the legislative history of the 1995 Act does state, “[T]he digital transmission of a sound recording that results in the reproduction by or for the transmission recipient of a phonorecord of that sound recording implicates the exclusive rights to reproduce and distribute the sound recording and the musical work embodied therein.” S. 128, 104th Cong., 1st Sess. 27 (1995), reprinted in 1995 U.S.C.C.A.N. 356, 374. As such, the 104th Congress well recognized that electronic transmissions implicate the distribution right in cases like this one.

CONCLUSION

For all of the foregoing reasons, unauthorized electronic transmissions of plaintiffs’ copyrighted sound recordings violate the exclusive right of distribution under the Copyright Act, and plaintiffs have properly stated a claim for violations of that right.

Dated: New York, New York
March 3, 2006

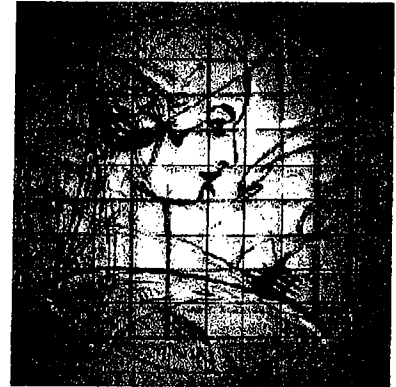
COWAN, LIEBOWITZ & LATMAN, P.C.
Attorneys for Plaintiffs

By: s/ J. Christopher Jensen
J. Christopher Jensen (JJ-1864)
Maryann Penney (MP-0741)
1133 Avenue of the Americas
New York, NY 10036-6799
Phone: (212) 790-9200
Fax: (212) 575-0671

HOLME ROBERTS & OWEN LLP
Richard L. Gabriel (RG-05065)
1700 Lincoln, Suite 4100
Denver, Colorado 80203
Phone: (303) 861-7000
Fax; (303) 866-0200

C O P Y R I G H T L A W

Peer-to-Peer File Sharing and Copyright Law after Napster



*Fred von Lohmann/senior staff attorney (fair use & intelletual property)
January 2003*

What this is, and who should read it.

As the Napster saga illustrates, the future of peer-to-peer file-sharing is entwined, for better or worse, with copyright law. The legal fight has already broken out, with copyright owners targeting not only the makers of file-sharing clients like Napster, Scour, Audiogalaxy, Aimster and Kazaa, and Morpheus, but also companies that provide products that rely on or add value to public P2P networks, such as MP3Board.com, which provides a web-based search interface for the Gnutella network.

The fight has only just begun. If these early skirmishes yield any lesson for future P2P developers, it's that a legal strategy needs to be in place early, preferably at the beginning of development, rather than bolted on at the end. As a result, if you are interested in peer-to-peer file sharing, whether as a developer, investor, or provider of ancillary services (such as search services, platform tools, or security), it's time to bone up on some copyright law basics.

This piece is meant as a general explanation of the U.S. copyright law principles most relevant to P2P file-sharing technologies. It is aimed primarily at:

- **Developers of core P2P file-sharing technology, such as the underlying protocols, platform tools, and specific client implementations;**
- **Developers of ancillary services that depend upon or add value to P2P file-sharing networks, such as providers of search, security, metadata aggregation, and other services;**
- **Investors seeking to evaluate the potential copyright risks associated with the various ventures listed above.**

The following discussion is meant as a general introduction, and thus occasionally glosses over some of copyright law's more subtle nuances. At the most basic level, it is aimed not at giving you all the answers, but rather at allowing you to recognize the right questions to ask your lawyers.

What this is not: The following discussion focuses only on U.S. copyright law, and does not address any issues that may arise under non-U.S. law. While non-copyright principles may also be mentioned, this discussion does not attempt to examine other legal principles that might apply to P2P file-sharing, including patent, trademark, trade secret, or unfair competition. Nothing contained herein constitutes legal advice—please discuss your individual situation with your own attorney.

Copyright Basics and the Intersection with P2P Filesharing

Copyright law applies to virtually every form of expression that can be captured (or, to use the copyright term of art, "fixed") in a tangible medium, such as on paper, film, magnetic tape, hard drive, optical media, or even merely in RAM. Songs, books, photographs, software, and movies are all familiar examples of copyrighted works. Copyright protection

begins from the moment that the expression is fixed, and continues for the lifetime of the author, plus 70 years.

During this period, copyright law reserves certain rights exclusively to the owner of the work, including the right to reproduce, distribute, and publicly perform the work. So, for example, if you wrote a song and recorded it on your computer, you would own the resulting copyrighted work and only you would have the right to make copies of the file, distribute it to the public, or sing the song in your local concert hall. If anyone else did any of these things without your permission, she would be infringing your copyright (unless the activity qualified as a "fair use" or fell into one of the other statutory exceptions to a copyright owner's exclusive rights).

The nature of digital file-sharing technology inevitably implicates copyright law. First, since every digital file is "fixed" for purposes of copyright law (whether on a hard drive, CD, or merely in RAM), the files being shared generally qualify as copyrighted works. Second, the transmission of a file from one person to another results in a reproduction, a distribution, and possibly a public performance (in the world of copyright law, "public performance" includes the act of transmitting a copyrighted work to the public). To a copyright lawyer, every reproduction, distribution, and public performance requires an explanation, and thus file-sharing systems seem suspicious from the outset.

The end-users: "direct" infringement.

For the individuals who are sharing files, the question becomes whether all of these reproductions, distributions, and public performances are authorized by the copyright owner or otherwise permitted under copyright law (as "fair use," for example). So, if the files you are sharing with your friends are videos of your vacation, you are the copyright owner and have presumably authorized the reproduction, distribution, and performance of the videos. However, if you are

sharing MP3's of Metallica's greatest hits, or disc images of the latest Microsoft Office 2000 installation CD, the issue becomes more complicated. In that case, assuming that the copyright owner has not authorized the activity, the question of copyright infringement will depend whether you can qualify for any of the limited exceptions to the copyright owner's exclusive rights. If not, you're what copyright lawyers call a "direct infringer"—you have directly violated one or more of the copyright owner's exclusive rights.

In a widely-used public peer-to-peer file-sharing environment, it is a virtual certainty that at least some end-users are engaged in infringing activity (unless specific technical measures are taken to prevent this, like permitting only the sharing of files that have been cryptographically marked as "authorized"). When the major record labels and music publishers decided to sue Napster, for example, it was not difficult for them to locate a large number of Napster users who were sharing copyrighted music without authorization.

The P2P tool maker: "contributory" and "vicarious" infringement.

But what does this have to do with those who develop and distribute peer-to-peer file-sharing tools? After all, in a pure peer-to-peer file-sharing system, the vendor of the file-sharing tool has no direct involvement in the copying or transmission of the files being shared. These activities are handled directly between end-users.

Copyright law, however, can sometimes reach beyond the direct infringer to those who were only indirectly involved in the infringing activity. As in many other areas of the law (think of the "wheel man" in a stick up, or supplying a gun to someone you know is going to commit a crime), copyright law will sometimes hold one individual accountable for the actions of another. So, for example, if a swapmeet owner rents space to a vendor with the knowledge that the vendor sells counterfeit CDs, the swapmeet owner can be held liable for infringement alongside the vendor.

Under copyright law, this indirect, or "secondary," liability can take two distinct forms: contributory infringement and vicarious infringement.

Contributory Infringement

Contributory infringement is similar to "aiding and abetting" liability: one who knowingly contributes to another's infringement may be held accountable. Or, as the courts have put it, "one who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, may be held liable as a contributory infringer." So, in order to prevail on a contributory infringement theory, a copyright owner must prove each of the following elements:

- Direct Infringement: There has been a direct infringement by someone.**
- Knowledge: The accused contributory infringer knew of the underlying direct infringement. This element can be satisfied by showing either that the contributory infringer actually knew about the infringing activity, or that he reasonably should have known given all the facts and circumstances. At a minimum, however, the contributory infringer must have some specific information about infringing activity—the mere fact that the system is capable of being used for infringement, by itself, is not enough.**
- Material Contribution: The accused contributory infringer induced, caused, or materially contributed to the underlying direct infringement. Merely providing the "site and facilities" that make the direct infringement possible can be enough.**

Vicarious Infringement

Vicarious infringement is derived from the same legal principle that holds an employer responsible for the actions of its employees. A person will be liable for vicarious infringement if he has the right and ability to supervise the direct infringer and also has a direct

financial interest in his activities. Thus, in order to prevail on a vicarious infringement theory, a copyright owner must prove each of the following:

- **Direct Infringement:** There has been a direct infringement by someone.
- **Right and Ability to Control:** The accused vicarious infringer had the right and ability to control or supervise the underlying direct infringement. This element does not set a high hurdle. For example, the Napster court found that the ability to terminate user accounts or block user access to the system was enough to constitute "control."
- **Direct Financial Benefit:** The accused vicarious infringer derived a "direct financial benefit" from the underlying direct infringement. In applying this rule, however, the courts have not insisted that the benefit be especially "direct" or "financial"—almost any benefit seems to be enough. For example, the Napster court found that "financial benefit exists where the availability of infringing material acts as a draw for customers" and the growing user base, in turn, makes the company more attractive to investors.

The nature of vicarious infringement liability creates a strong incentive to monitor the conduct of your users. This stems from the fact that knowledge is not required for vicarious infringement liability; a person can be a vicarious infringer even if they are completely unaware of infringing activity.

As a result, if you exercise control over your users and derive a benefit from their activities, you remain ignorant of their conduct at your own risk. In the words of the Napster court, "the right to police must be exercised to the fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability."

Indirect Liability and P2P Systems: the Napster Case

The Napster case represents the leading case

applying these indirect liability theories to a peer-to-peer file-sharing service. In that case, the plaintiffs admitted that Napster did not, itself, make or distribute any or their copyrighted works. Instead, they argued that Napster is liable for contributory and vicarious infringement. Based on these theories, the plaintiffs convinced a federal district court to grant a preliminary injunction against Napster. That ruling was appealed and affirmed by the Ninth Circuit Court of Appeals. In its February 12, 2001 opinion, the Ninth Circuit rejected each of Napster's proposed defenses.

Turning first to contributory infringement, the Ninth Circuit upheld the lower court's findings:

- **Direct Infringement:** At least some Napster users are direct infringers, because they distributed and reproduced copyrighted music without authorization.
- **Knowledge:** Napster had actual knowledge of infringing activity, based on internal company emails and the list of 12,000 infringing files provided by the RIAA. Moreover, Napster should have known of the infringing activity, based on the recording industry experience and downloading habits of its executives and the appearance of well-known song titles in certain promotional screen shots used by Napster.
- **Material Contribution:** Napster provided the "site and facilities" for the directly infringing conduct of its users.

The Ninth Circuit also endorsed the lower court's vicarious infringement analysis:

- **Direct Infringement:** At least some Napster users are direct infringers, because they distributed and reproduced copyrighted music without authorization.
- **Right and Ability to Control:** Napster has the ability to control the infringing activity of its users because it retains the right to block a user's ability to access its system.
- **Financial Benefit:** Napster derived a financial

benefit from the infringing activities of its users because this activity acted as a "draw" for customers, and a portion of Napster's value is derived from the size of its user base.

The Ninth Circuit concluded, however, that the lower court had not adequately considered the technological limits of the Napster system when crafting the preliminary injunction. In ordering the district court to revise its injunction, the Ninth Circuit spelled out some guiding principles. First, in order to prevent contributory infringement, after receiving notice from a copyright owner that a work is being shared on its system without authorization, Napster was required to take reasonable steps to prevent further distribution of the work. Ultimately, Napster implemented a number of filtering mechanisms (including file name filters and acoustic fingerprinting filters) intended to filter out works that were not approved for sharing. Unfortunately, these filters were never accurate enough to satisfy the district court judge, and Napster ended up in bankruptcy before a trial could be held.

Second, in order to prevent vicarious infringement, the Ninth Circuit declared that "Napster... should bear the burden of policing its system within the limits of the system." During the period until its bankruptcy, Napster and the plaintiffs bitterly disagreed about what these monitoring obligations entailed. At a minimum, Napster had the duty to terminate users who were identified as infringers. Beyond that, there was little agreement. The disagreement was never fully resolved by the court, since Napster was shut down while it worked on improving its filtering technologies.

Potential Defenses Against Contributory and Vicarious Liability

No Direct Infringer: "All of My Users are Innocent"

If there is no direct infringement, there can be no indirect liability. Consequently, if a peer-to-peer developer can plausibly claim that no users in the network are sharing copyrighted works without

authorization, this would be a complete defense to any contributory or vicarious infringement claims. Unfortunately, this may be extremely difficult to demonstrate, given the decentralized nature of most P2P networks and the wide variety of uses to which they may be put. Even if file sharing by some users is privileged under the "fair use" doctrine or another statutory exception to copyright, it will be very difficult to show that every user falls within such an exception. Nevertheless, in certain specialized networks that permit the sharing of only secure, authorized file types, this may be a viable defense.

The Betamax defense: "Capable of substantial noninfringing uses"

Holding technology developers responsible for the unlawful acts of end-users obviously can impose a crushing legal burden on those who make general-purpose tools. Fortunately, the Supreme Court has defined an outer limit to copyright's indirect liability theories.

In a case involving the Sony Betamax VCR, the Supreme Court found that contributory infringement liability could not reach the manufacturer of a device that is "capable of substantial noninfringing use." In that case, the Court found that the VCR was capable of several noninfringing uses, including the time-shifting of television broadcasts by home viewers. In the Court's view, it does not matter what proportion of the uses are noninfringing, only whether the technology is "capable" of substantial noninfringing uses.

Unfortunately, the "Betamax defense" has been under sustained legal attack in the cases involving P2P technology. In the Napster case, the court found that this defense does not apply at all to vicarious liability. Accordingly, if you have control over, and derive a financial benefit from, direct infringement, the existence of "substantial noninfringing uses" for your service is irrelevant.

Moreover, the Napster court concluded that the

Betamax defense may only apply until the copyright owner notifies you regarding specific infringing activity by end-users. At that point, a failure to act to prevent further infringing activity will give rise to liability, and the existence of "substantial noninfringing uses" becomes irrelevant.

The "Betamax defense" has also come under attack in the Aimster case, where a court stated that the defense was not available where the technology is primarily used for infringement. (This notwithstanding the fact that the "proportion of uses" test was explicitly rejected in the Supreme Court's Betamax ruling.) The scope of the "Betamax defense" is also at the heart of the case against Kazaa, Morpheus and Grokster, currently pending in Los Angeles.

The recent court interpretations of the "Betamax defense" have at least two important implications for P2P developers. First, it underscores the threat of vicarious liability—at least in the Ninth Circuit, a court will not be interested in hearing about your "substantial noninfringing uses" if you are accused of vicarious infringement. Accordingly, "control" and "direct financial benefit," as described above, should be given a wide berth.

This will likely reduce the attractiveness of business models built on an on-going "service" or "community-building" model, to the extent that these models allow the provider to control user activity (i.e., terminate or block users) and create value by attracting a large user base.

Second, with respect to contributory infringement, the recent interpretations of the Betamax defense suggest that, once you receive specific notices from copyright owners about infringing activities, your "substantial noninfringing uses" may no longer serve as a complete shield to contributory liability. The risk then arises that a developer may have a legal duty to "do something" about the infringing activities.

But what "something" must be done? The Napster

decision recognizes that the ability to respond to these notices may be limited by the technology behind the challenged service or product. In cases involving decentralized P2P networks, there may be nothing a software developer can do to stop future infringements (just as Xerox cannot control what a photocopier is used for after it is sold).

Nevertheless, copyright owners are arguing that technologists should have a duty to redesign technologies once they are put on notice regarding infringing end-users. What this might entail is difficult to predict, but may include, in some cases, modification of the architecture and capabilities of the tool, service or system.

The exact contours of the Betamax defense are still being developed in the courts, some of which seem to have embraced conflicting interpretations. Breaking developments on this front may have important ramifications for P2P developers and should be closely monitored.

The DMCA Section 512 "safe harbors"

In 1998, responding in part to the concerns of ISPs regarding their potential liability for the copyright infringement of their users, Congress enacted a number of narrow "safe harbors" for copyright liability. These safe harbors appear in section 512 of the Copyright Act, which in turn appears in title 17 of the U.S. Code (17 U.S.C. 512). These safe harbors apply only to "online service providers," and only to the extent that the infringement involves four functions: transitory network transmissions, caching, storage of materials on behalf of users (e.g., web hosting, remote file storage), and the provision of information location tools (e.g., providing links, directories, search engines).

Each of these functions, however, is narrowly defined by the statute (e.g., they don't cover what you'd think) and reflects the state of the art in 1998. For example, the automated web page caching conducted by AOL in 1998 falls within the caching safe harbor,

while the more sophisticated efforts of Akamai today may not. Because Congress did not anticipate peer-to-peer file sharing when it enacted the safe harbors, many P2P products may not fit within the four enumerated functions. For example, according to an early ruling by the district court in the Napster case, an OSP cannot use the "transitory network transmission" safe harbor unless the traffic in question passes through its own private network. Many P2P products will, by their very nature, flunk this requirement, just as Napster did.

In addition to being limited to certain narrowly-circumscribed functions, the safe harbors are only available to entities that comply with a number of complex, interlocking statutory requirements:

- The online service provider ("OSP") must (1) adopt, reasonably implement, and notify its users of a policy of terminating the accounts of subscribers who are repeat infringers; and (2) accommodate and not interfere with "standard technical measures" that have been widely adopted on the basis of industry-wide consensus (e.g., the use of robot.txt exclusion headers to block spiders).
- The OSP must designate a "copyright agent" to receive notices of alleged copyright infringement, register the agent with the Copyright Office, and place relevant contact information for the agent on its web site.
- The OSP must, upon receiving a notification of infringement from a copyright owner, expeditiously remove or disable access to the infringing material ("notice and takedown").
- The OSP must not have known about the infringement, or been aware of facts from which such activity was apparent (i.e., if you take a "head in the sand" approach, you lose the safe harbor).
- The OSP must not receive a direct financial benefit from infringing activity, in a situation where the OSP controls such activity (i.e., if you're liable for vicarious liability, the safe harbor may not protect you).

In the final analysis, qualifying for any of the DMCA safe harbors requires careful advance attention to the legal and technical requirements and obligations that the statute imposes. As a result, any P2P developer who intends to rely on them should seek competent legal counsel at an early stage of the development process—an after-the-fact, "bolt on" effort to comply is likely to fail (as it did for Napster).

The DMCA ban on circumvention technologies

One recent addition to the copyright landscape deserves special attention. Section 1201 of the Copyright Act, enacted as part of the DMCA, makes it unlawful to "circumvent" any technology aimed at protecting a copyrighted work. In addition, the development, distribution or use of circumvention technology or devices is, with only narrow exceptions, also unlawful. For example, if a copyright owner uses a digital rights management ("DRM") solution to protect a song, it would be unlawful for anyone to crack the encrypted file without the copyright owner's permission, or to build or distribute a software tool designed to crack the file. The litigation involving DeCSS software, which is capable of decrypting video DVDs, represents one of the first cases testing these "anti-circumvention" provisions of the DMCA.

Of course, circumvention technology is not a necessary part of a peer-to-peer file-sharing network. Today's P2P protocols, such as Gnutella, simply facilitate file transfers, leaving the file itself, whether encrypted or not, unaltered. Nevertheless, as copyright owners begin to deploy DRM and watermarking systems, there may be interest in integrating circumvention tools with file-sharing tools. In light of the DMCA's broad ban on circumvention technology, however, any such integration may substantially increase the risk of liability.

Lessons and Guidelines for P2P Developers

A few general guidelines for P2P developers can

be derived from the discussion above. These are steps you can take that may: (1) reduce the chance that your project will be an easy, inviting target for copyright owners; (2) placate your investors when they ask you whether you are likely to spend their money on litigation rather than products; and (3) minimize the chances that your case will become the next legal precedent that content owners can use to threaten future innovators.

Of course, because the relevant legal principles are still in flux, these guidelines represent merely one, general analysis of the legal landscape—please consult with an attorney regarding your precise plans.

A. Make and store no copies.

This one may be obvious, but remember that if you make or distribute any copies (even if only in RAM) of copyrighted works, you may be held liable as a direct infringer. The court will not be interested in "control" or "knowledge" or "financial benefit" or "material contribution." If you made or transmitted copies, you're probably liable for infringement.

Of course, this shouldn't be a problem for most P2P developers, since the great insight of peer-to-peer architectures is that the actual resources being shared need not pass through any central server. Nevertheless, be careful where caching or similar activities are concerned.

B. Your two options: total control or total anarchy.

In the wake of recent decisions on indirect copyright liability, it appears that copyright law has foisted a binary choice on P2P developers: either build a system that allows for thorough monitoring and control over user activities, or build one that makes such monitoring and control completely impossible.

Contributory infringement requires that you have "knowledge" of, and "materially contribute" to,

someone else's infringing activity. In most cases, it will be difficult to avoid "material contribution"—after all, if your system adds any value to the user experience, a court may conclude that you have "materially contributed" to any infringing user activities.

So the chief battleground for contributory infringement will likely be the "knowledge" issue. The applicable legal standards on this question are still very much in dispute —especially as relates to the "Betamax defense." The Napster court's analysis suggests that once you receive notice that your system is being used for infringing activity (e.g., a "cease and desist" letter from a copyright owner), you have a duty to "do something" to stop it.

What might that "something" be? Well, it should be limited by the architecture of your system, but may ultimately be decided by a court. So, in order to avoid the unpleasant surprise of a court telling you to re-engineer your technology to stop your infringing users, you can either include mechanisms that enable monitoring and control of user activities (and use them to stop allegedly infringing activity when you receive complaints), or choose an architecture that will convince a judge that such monitoring and control is impossible. (Copyright owners have begun arguing that you must at least redesign future versions of your software to prevent infringement. This remarkable argument has not yet been accepted by any court.)

The Napster court's vicarious liability analysis also counsels for either a total control or total anarchy approach. Vicarious liability requires that you "control," and receive "benefit" from, someone else's infringing activity. The "benefit" element will be difficult to resist in many P2P cases (at least for commercial products)—so long as the software permits or enables the sharing of infringing materials, this will serve as a "draw" for

users, which can be enough "benefit" to result in liability.

So the fight will likely center on the "control" element. The Napster court found that the right to block a user's access to the service was enough to constitute "control." The court also found that Napster had a duty to monitor the activities of its users "to the fullest extent" possible. Accordingly, in order to avoid vicarious liability, a P2P developer would be wise to either incorporate mechanisms that make it easy to monitor and block infringing users, or choose an architecture that will convince a judge that monitoring and blocking is impossible.

- c. Better to sell stand-alone software products than on-going services.**

Vicarious liability is perhaps the most serious risk facing P2P developers. Having the power to terminate or block users constitutes enough "control" to justify imposing vicarious liability. Add "financial benefit" in the form of a business model that depends on a large user base, and you're well on your way to joining Napster as a vicarious infringer. This is true even if you are completely unaware of what your users are up to—the pairing of "control" and "financial benefit" are enough.

Of course, most "service" business models fit this "control" and "benefit" paradigm. What this means is that, after the Napster decision, if you offer a "service," you may have to monitor your users if you want to escape liability. If you want to avoid monitoring obligations, you'll have to give up on "control."

Vendors of stand-alone software products may be in a better position to resist monitoring obligations and vicarious infringement liability. After Sony sells a VCR, it has no control over what the end-user does with it. Neither do the makers of

photocopiers, optical scanners, or audio cassette recorders. Having built a device with many uses, only some of which may infringe copyrights, the typical electronics manufacturer has no way to "terminate" end-users or "block" their ability to use the device. The key here is to let go of any control you may have over your users—no remote kill switch, automatic updates feature, contractual termination rights, or other similar mechanisms.

D. Can you plausibly deny knowing what your end-users are up to?

Assuming that you have escaped vicarious infringement by eliminating "control" or "financial benefit," there is still the danger of contributory infringement. To avoid liability here, you will need to address whether you knew, or should have known, of the infringing activity of your users.

Have you built a level of "plausible deniability" into your product architecture and business model? If you promote, endorse, or facilitate the use of your product for infringing activity, you're asking for trouble. Similarly, software that sends back usage reports may lead to more knowledge than you want. Customer support channels can also create bad "knowledge" facts. Instead, talk up all the great legitimate capabilities, sell it (or give it away), and then leave the users alone. Again, your choices are total control, or total anarchy.

E. What are your substantial noninfringing uses?

If your product is intended to work solely (or best) as a mechanism for copyright piracy, you're asking for legal trouble. More importantly, you're thinking too small. Almost all peer-to-peer systems can be used for many different purposes, some of which the creators themselves fail to appreciate.

So create a platform that lends itself to many uses. Actively, sincerely, and enthusiastically promote

the noninfringing uses of your product. Gather testimonials from noninfringing users. The existence of real, substantial noninfringing uses will increase the chances that you can invoke the "Betamax defense" if challenged in court.

F. Do not promote infringing uses.

Do not promote any infringing uses. Be particularly careful with marketing materials and screenshot illustrations—entertainment company attorneys are very good at making hay out of the fact that Beatles songs were included in sample screenshots included in marketing materials or documentation. Have an attorney review these materials closely.

G. Disaggregate functions.

Separate different functions and concentrate your efforts on a discrete area. In order to be successful, peer-to-peer networks will require products to address numerous functional needs—search, namespace management, security, dynamic file redistribution—to take a few examples. There's no reason why one entity should try to do all of these things. In fact, the creation of an open set of protocols, combined with a competitive mix of interoperable, but distinct, applications is probably a good idea from a product-engineering point of view.

This approach may also have legal advantages. If Sony had not only manufactured VCRs, but also sold all the blank video tape, distributed all the TV Guides, and sponsored clubs and swap meets for VCR users, the Betamax case might have turned out differently. Part of Napster's downfall was its combination of indexing, searching, and file sharing in a single piece of software. If each activity is handled by a different product and vendor, on the other hand, each entity may have a better legal defense to a charge of infringement.

A disaggregated model, moreover, may limit what a court can order you to do to stop infringing activity by your users. As the Napster court recognized, you can only be ordered to police your own "premises"—the smaller it is, the less you can be required to do.

Finally, certain functions may be entitled to special protections under the "safe harbor" provisions of the Digital Millennium Copyright Act ("DMCA"). Search engines, for example, enjoy special DMCA protections. Thus, the combination of a P2P file sharing application with a third party search engine might be easier to defend in court than Napster's integrated solution.

H. Don't make your money from the infringing activities of your users.

Avoid business models that rely on revenue streams that can be directly traced to infringing activities. For example, a P2P file-sharing system that includes a payment mechanism might pose problems, if the system vendor takes a percentage cut of all payments, including payments generated from sales of bootleg Divx movie files.

I. Give up the EULA

Although end-user license agreements ("EULAs") are ubiquitous in the software world, copyright owners have used them in P2P cases to establish "control" for vicarious liability purposes. On this view, EULAs represent "contracts" between vendors and their users, and thus give software vendors legal control over end-user activities. EULAs that permit a vendor to terminate at any time for any reason may raise particular concerns, insofar as they leave the impression that a vendor has the legal right to stop users from using the software.

P2P software vendors should consider

distributing their code without a EULA. Even without a EULA, a software developer retains all of the protections of copyright law to prevent unauthorized duplication and modifications.

J. No "auto-updates"

Stay away from any "auto-update" features that permit you to automatically patch, update, or otherwise modify software on the end-user's machine. Copyright owners have argued that these features establish "control" for vicarious liability purposes (on the theory that you can always "update" software to prevent its use for infringement, by retrofitting acoustic filtering, for example).

At a minimum, users should always retain the ability to decline any update. Control should rest in the end-user's hands, not the software vendor's (this as much for security reasons as legal reasons).

K. No customer support.

Any evidence that you have knowingly assisted an end-user in committing copyright infringement will be used against you. In the P2P cases so far, one source for this kind of evidence is from customer support channels, whether message board traffic or email. A user writes in, explaining that the software acted strangely when he tried to download The Matrix. If you answer him, copyright owners will make it seem that you directly assisted the user in infringement, potentially complicating your contributory infringement defense.

Even if you read the message but don't answer, or answer in a general FAQ, copyright owners may argue that support requests were enough to create "knowledge" of infringing activities.

So let the user community support themselves in

whatever forums they like. Keep your staff out of it. (This will be easier if you are open source, of course.)

L. Be open source.

In addition to the usual litany of arguments favoring the open-source model, the open source approach may offer special advantages in the peer-to-peer realm. It may be more difficult for a copyright owner to demonstrate "control" or "financial benefit" with respect to an open source product. After all, anyone can download and compile open source code, and no one has the ability to "terminate" or "block access" or otherwise control the use of the resulting applications.

"Financial benefit" may also be a problematic concept where the developers do not directly realize any financial gains from the code (as noted above, however, the Napster court has embraced a very broad notion of "financial benefit," so this may not be enough to save you). Finally, by making the most legally dangerous elements of the P2P network open source (or relying on the open source projects of others), you can build your business out of more legally defensible ancillary services (such as search services, bandwidth enhancement, file storage, file meta-data services, etc.).

Good luck, and change the world!

*** * ***

About the Author: Fred von Lohmann is a senior staff attorney with the Electronic Frontier Foundation, specializing in intellectual property issues. In that role, he has represented programmers, technology innovators, and individuals in litigation against every major record label, movie studio, and television network

(as well as several cable TV networks and music publishers) in the United States. In additon to litigation, he is involved in EFF's efforts to educate policy-makers regarding the proper balance between intellectual property protection and the public interest in fair use, free expression, and innovation.

Copyright Information: Permission to reproduce and distribute this paper is freely given, provided that such activities are for noncommercial purposes and include attribution to the author. All other rights reserved. Contact the author at fred@eff.org for all other permissions.

© 2003 EFF v. 2.0



HOMEPAGE

[Home Page](#) | [About Us](#) | [E-Mail Us](#) | [P2P Offshore](#) | [THINGS](#) | [P2P File Sharing](#) | [Site Map](#)



DMCA Section 104 Report

**U.S. Copyright Office
August 2001**

**A Report of the Register of Copyrights
Pursuant to §104 of the Digital Millennium Copyright Act**

archival exemption as articulated by CONTU.²⁶⁸ Accordingly, we conclude that the evidence at this time of an effect of title I of the DMCA on the operation of section 117 is not substantial, and no legislative change is warranted.

B. THE EFFECT OF ELECTRONIC COMMERCE AND TECHNOLOGICAL CHANGE ON SECTIONS 109 AND 117

We have made no attempt in preparing this study to separate out the impact of electronic commerce on sections 109 and 117 from the impact of technological change. Such an effort would probably have been futile since, as the language of section 104 suggests, by grouping the two issues together, the issues are inextricably intertwined. In its essence, electronic commerce is commerce carried out through new technologies. This study is an outgrowth of the intersection between new technology and the new business models that it makes possible. Our evaluation is of the impact of that intersection on the specified provisions of the Copyright Act.

1. The First Sale Doctrine in the Digital World

a. Application of Existing Law to Digital Content

The application of section 109 to digital content is not a question of whether the provision applies to works in digital form — it does. Physical copies of works in a digital format, such as CDs or DVDs, are subject to section 109 in the same way as physical copies of works in analog form. Likewise, a lawfully made tangible copy of a digitally downloaded work, such as an image file downloaded directly to a floppy disk, is subject to section 109. The question we address here

²⁶⁸ See *supra*, at 29.

is whether the conduct of transmitting the work digitally,²⁶⁹ so that another person receives a copy of the work, falls within the scope of the defense.²⁷⁰

Section 109 limits a copyright owner's exclusive right of distribution. It does not, by its terms, serve as a defense to a claim of infringement of any of the other exclusive rights.²⁷¹ The transmissions that are the focus of proposals for a "digital first sale doctrine"²⁷² result in reproductions of the works involved. The ultimate product of one of these digital transmissions is a new copy in the possession of a new person. Unlike the traditional circumstances of a first sale transfer, the recipient obtains a new copy, not the same one with which the sender began. Indeed, absent human or technological intervention, the sender retains the source copy. This copying implicates the copyright owner's reproduction right as well as the distribution right.

²⁶⁹ The transmissions discussed in this section are not broadcasts, but transmissions that, like point-to-point transmissions, involve the selection of specific recipients by the sender.

²⁷⁰ Some commenters were confused between the proposal to apply the first sale doctrine to otherwise unauthorized digital transmissions of copyrighted works by lawful owners of copies of such works and the notion that a lawful copy created as a result of an authorized digital transmission is a lawful copy for purposes of section 109. The former would expand the scope of section 109 and will be discussed below. The latter is well within the current language of the statute. Regardless of whether a copy is created as a result of the nearly instantaneous transmission of digital information through broadband computer connections or as a result of months of painstaking labor of a cloistered monk working with a quill by candlelight, so long as that copy is lawfully made, it satisfies the second prong of eligibility for the section 109 defenses.

²⁷¹ 17 U.S.C. § 109(a). In limited circumstances the public display right is covered as well. 17 U.S.C. § 109(c). *See supra*, note 53.

²⁷² The term "digital first sale doctrine" is used here to denote a proposed copyright exception that would permit the transmission of a work from one person to another, generally via the Internet, provided the sender's copy is destroyed or disabled (whether voluntarily or automatically by virtue of a technological measure). We use the term because it has been used frequently in discourse about the subject. It is, however, a misnomer since the proposal relates not to works in digital form generally (which are, of course, already subject to section 109), but to *transmissions* of such works.